BROCADE PRODUCT TRAINING

BCSM in a Nutshell
Study Guide for Exam 143-350

Revision 0308

Exam Preparation Materials

Brocade Education Services

©2008 Brocade Communications Systems, Inc.

BROCADE

Corporate Headquarters
San Jose, CA USA
T: (408) 333-8000
info@brocade.com

European Headquarters
Geneva, Switzerland
T: +41 22 799 56 40
emea-info@brocade.com

Asia Pacific Headquarters
Singapore
T: +65-6538-4700
apac-info@brocade.com

© 2008 Brocade Communications Systems, Inc. All Rights Reserved. 03/08

Brocade, the Brocade B-weave logo, Fabric OS, File Lifecycle Manager, MyView, Secure Fabric OS, SilkWorm, and StorageX are registered trademarks and the Brocade B-wing symbol and Tapestry are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. FICON is a registered trademark of IBM Corporation in the U.S. and other countries. All other brands, products, or service names are or may be trademarks or service marks of, and are used to identify, products or services of their respective owners.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

BROCADE

Brocade Certified SAN Manager

Welcome to the BCSM in a Nutshell 2008 edition.

Objective: We've put this guide together to help you prepare for the BCSM certification exam number 143-350. This exam tests SAN management skills using the following Brocade products:

- Brocade switches, routers and Directors running up through Fabric OS v5.3.0
- All licensed (software) features through Fabric OS v5.3.0
- M-EOS 9.6
- EFCM 9.5 and Fabric Manager 5.3
- ESCM
- SAN Health

Audience: This self-study guide is targeted for those who have attended the *CSM 264 Brocade 4 Gbit/sec Accelerated Brocade Certified SAN Manager* blended instructor-led training, and who wish to undertake self-study or review activities before taking the actual BCSM test. It is also for those individuals who do not have the time to attend the formal training, but who still wish to be certified as a BCSM. It is not intended as a substitute for classroom training, and hands-on time. We still highly recommend you attend the *CSM 264 Brocade 4 Gbit/sec Accelerated Brocade Certified SAN Manager* blended instructor-led course.

Usage: This guide summarizes the key topics on the BCSM exam for you in an easy-to-use format. It is organized closely around the exam objectives. Use the Table of Contents, List of Tables, and List of Figures to quickly jump to a given area.

We hope you find this guide useful in your journey towards BCSM Certification, and we welcome your feedback. Please email comments or feedback to jcannata@brocade.com

Helen Lautenschlager
Director of Education Services

Joe Cannata
Certification Manager

© 2008 Brocade Communications Systems, Incorporated.

TABLE OF CONTENTS

List of Tables 3
List of Figures 4
1 Security....5
1.1 Managing SAN Security....5
2 Management Tools....11
2.1 Implementing SAN Management Tools....11
3 Reporting and Documentation 18
3.1 SAN Documentation 18
3.2 Tools to Document a SAN....19
4 Troubleshooting 20
4.1 Methods & Tools for Troubleshooting and Data gathering....20
4.2 Identifying Information Required for Problem Escalation....25
5 SAN Monitoring 26
5.1 Identifying Tools to Monitor a SAN 26
5.2 How to Monitor and Manage Shared Devices Between Edge Fabrics 27
5.3 How to monitor and Manage Devices 29
6 SAN Configuration 32
6.1 Managing FICON fabrics....32
6.2 Performing Routine Maintenance 34
6.3 Maintaining SAN Extension Solutions....36
6.4 Managing Access Gateway Solutions 38
7 Taking the Test....41

© 2008 Brocade Communications Systems, Incorporated.

LIST OF TABLES

Table 1: Password Policy CLI Commands.....8
Table 2: Policy Distribution.....9
Table 3: BB Credits.....37

© 2008 Brocade Communications Systems, Incorporated.

LIST OF FIGURES

Figure 1: EFCM Routing 11
Figure 2: EFCM Group Manager 13
Figure 3: Fabric Merge Troubleshooting Tree 21
Figure 4: Marginal Link/Port Fault Troubleshooting Tree 23
Figure 5: Sample Routed Fabric 27
Figure 6: Active Zone Set Tab in EFCM 29
Figure 7: Supported FICON Topologies 32
Figure 8: Access Gateway 38
Figure 9: Access Gateway Default Port Map 39
Figure 10: Access Gateway 24-Bit FC Address Assignments 40
Figure 11: Introduction Screen 41
Figure 12: Non-disclosure Agreement 42
Figure 13: Sample Question 43
Figure 14: Examination Summary 44

© 2008 Brocade Communications Systems, Incorporated.

1 SECURITY

1.1 MANAGING SAN SECURITY

PROTECTING YOUR MANAGEMENT INTERFACES

A goal is to minimize threats by limiting access to the management interfaces. This can be achieved by:

- Employing IP network security best practices
- Disabling unused management interfaces like telnet, SNMP and HTTP
- Using secure protocols like SSL, SMNPv3 and SSHv2

BEST PRACTICES

Best-practice IT security strives to maintain five basic objectives that provide a foundation for protecting against threats and attacks that can be executed against a storage environment:

- Availability
  - Data must always be available to authorized users whenever it is needed
- Integrity
  - In order to maintain its integrity, data must not be modified in any way
- Authentication
- Confidentiality[3]
  - Sensitive data such as personal information, intellectual property, and data pertaining to national security must remain strictly confidential
- Non-repudiation of data
  - Non-repudiation is the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated. On the Internet, the digital signature is used not only to ensure that a message or document has been electronically signed by the person that purported to sign the document, but also, since a digital signature can only be created by one person, to ensure that a person cannot later deny that they furnished the signature.

When implementing SAN-attached servers located in a DMZ, Brocade recommends the following to protect the SAN from the Internet:

- Use a VLAN for the management network
- Create a separate zone for the devices in the DMZ
- Implement LUN masking at the disk storage controller

© 2008 Brocade Communications Systems, Incorporated.

ADDITIONAL BEST PRACTICES

- Implement the Track Changes feature in Fabric OS to see who logged in and when, and it reports them as messages in the RASlog
- Restrict responsibilities by assigning a different user name to each SAN administrator and a specific role using Role-Based Access Controls (RBAC)
- Use Virtual Fabrics and Fibre Channel routing
- Use a login banner to provide legal support
- Manage multiple user accounts with RADIUS for centralized login management

RBAC IN FABRIC OS V5.3

- user – view only privileges
- zoneadmin - can perform zone operations only
- basicswitchadmin - can do mostly monitoring with very limited switch (local) command capability
- operator - can perform operations typically required during “off-hours” when an Admin is not present
- switchadmin – can perform most operations not involving security
- fabricadmin - can perform all operations except user and Virtual Administrative Domain (AD)
- securityadmin – grants permission for all security-related configuration operations only
- admin – the only role that can manage all features

SECURE PROTOCOLS

- SCP for firmware downloads and also for configuration file uploads/downloads
- HTTPS (requires a digital certificate) for Web Tools
- SSL in lieu of telnet
- SNMPv3 (but does not use a reliable transport protocol)
- IPsec for FCIP tunnels

PASSWORD STRENGTHENING POLICIES

- Account lockout
- Password expiration
- Password strength
- Password history

© 2008 Brocade Communications Systems, Incorporated.

ACCOUNT LOCKOUT POLICY

- Disables a user account when the user exceeds a configurable number of failed login attempts
- Policy can be configured to:
  - Keep account locked until explicit administrative action is taken
  - Automatically unlock after a specified duration
- Administrator may unlock a locked account at any time

PASSWORD EXPIRATION POLICY

- Forces expiration of a password after a configurable period of time
- When a password expires, user must change the password to complete the authentication process and open a user session
- A warning that password expiration is approaching is displayed when user logs in
- Number of days prior to expiration is a configurable parameter
- Password expiration policy is enforced across all user accounts except the root and factory accounts

PASSWORD STRENGTH POLICY

- Enforces a set of rules that new passwords must satisfy
- Is enforced across all user accounts
- Is enforced only when a new password is defined
- Configurable attributes
  - Minimum number of lowercase and uppercase alphabetic characters
  - Minimum number of numeric digits in the password
  - Minimum number of punctuation characters in the password
  - Minimum password length may be set from 8-40 characters
  - Maximum number of repeated characters
  - Maximum number of sequential characters

PASSWORD HISTORY POLICY

- Specifies the number of past password values that are disallowed when setting a new password
- A value of 1-24 may be specified (default value is 1)
- Prevents reuse of recently used passwords
- The password history policy is enforced only when a new password is defined
- Password history policy is enforced across all user accounts

© 2008 Brocade Communications Systems, Incorporated.

Password Strength Policy	
To set minimum lower case characters	passwdcfg --set -lowercase <value>
To set minimum uper case characters	passwdcfg --set -uppercase <value>
To set minimum number of digit	passwdcfg --set -digits <value>
To set minimum punctuation characters	passwdcfg --set -punctuation <value>
To set minimum password length	passwdcfg --set -minlength <value>
To set minimum character repeat	passwdcfg --set -repeat <value>
To set minimum character sequence	passwdcfg --set -sequence <value>
Password History Policy	
To set the password history	passwdcfg --set -history <value>
Password Expiration Policy	
To set a minimum password age	passwdcfg --set -minpasswordage <value>
To set a maximum password age	passwdcfg --set -maxpasswordage <value>
To set the password expiration warning	passwdcfg --set -warning <value>
Lockout Policy	
To set a lockout threshold policy	passwdcfg --set -lockoutthreshold <value>
To specify the lockout duration	passwdcfg --set -lockoutduration <value>
To disable admin account locking	passwdcfg --disableadminlockout
To enable admin account locking	passwdcfg --enableadminlockout
To manually unlock a locked account	userconfig --change <account name> -u

Table 1: Password Policy CLI Commands

BASE FABRIC OS V5.3 SECURITY POLICIES IN THE LOCAL SWITCH DATABASE

- Fabric Configuration Server (FCS):
  - Restricts which switches can change the configuration of the fabric
  - Basically an access control list
- Device Connection Control (DCC):
  - Restricts which Fibre Channel device ports can connect to which Fibre Channel switch ports
  - A violation will disable the port and generate a trap
  - Prevents host WWN spoofing attacks
- Switch Connection Control (SCC):
  - Restricts which switches can join a fabric
  - Only one SCC Policy may exist in the fabric
- IP Filter Policy (IPFILTER):
  - Filters IP management interface traffic; controls the access to management interfaces
- Fabric Element Authentication Policy (AUTH):
  - Authenticates switch-switch and/or device-switch connections
- Password database and user policy (PWD):
  - Enables users and passwords configured on one switch to be distributed to other switches

© 2008 Brocade Communications Systems, Incorporated.

POLICY DISTRIBUTION

- Each switch can be set to Accept or Reject individual security policies
- The policies are manually distributed to fabric switches
- Fabric Wide Consistency Policy (Absent/Tolerant/Strict)
  - Each fabric could have a consistency policy that would require automatic distribution of the SCC and DCC policies only
  - The PWD, IPFILTER, FCS, AUTH policies can only be manually distributed

Distribution Setting	Fabric-Wide Consistency Policy set to:		
	Absent	**Tolerant**	**Strict**
Reject	Database is protected - cannot be overwritten. Might not match other databases in the fabric.	Database is protected - cannot be overwritten. Might not match other databases in the fabric.	Database is protected - cannot be overwritten. Might not match other databases in the fabric.
Accept (default)	• Database is not protected - can be overwritten. • If the switch initiating the distribute has a strict or tolerant fabric-wide policy, the switch-local database can be overwritten by a distribute command • Active database may not always match other databases in the fabric	• Database is not protected • Fabric may contain switches running Fabric OS v5.1.x and earlier • Automatically distributes activated changes to other Fabric OS v5.2 switches • Active database may not always match other databases in the fabric	• Database is not protected • Fabric can only contain switches running Fabric OS v5.2.0 or higher • Automatically distributes activated changes to all switches in the fabric • Active database is the same for all switches in the fabric

Table 2: Policy Distribution

© 2008 Brocade Communications Systems, Incorporated.

DH-CHAP

Fabric OS v5.3.0 uses DH-CHAP and FCAP protocols for authentication

- Protocols use shared secrets and digital certificates to authenticate
- By default the switch attempts FCAP authentication first and DH-CHAP second
- The switch may be configured to negotiate FCAP, DH-CHAP or both

The AUTH policy supports two types of authentication policies

- E_Port authentication (used for switch-switch)
- Device authentication (used for device-switch)

EFCM STANDARD - AUTHENTICATION AND ENCRYPTION

A SAN manager can choose from two methods for authentication

- A SAN management application
- LDAP

Client-to-server authentication is done via Triple DES encryption, not MD5. This has no impact on SSL.

- If SSL is turned on, then the user password is sent from the client to the server in Triple DES encryption under the SSL socket
- If SSL is turned off, then the password is sent in Triple DES encryption, but not under SSL socket

The user authentication is never done with passwords sent in clear text across the network.

© 2008 Brocade Communications Systems, Incorporated.

2 MANAGEMENT TOOLS

2.1 IMPLEMENTING SAN MANAGEMENT TOOLS

EFCM AND ROUTING

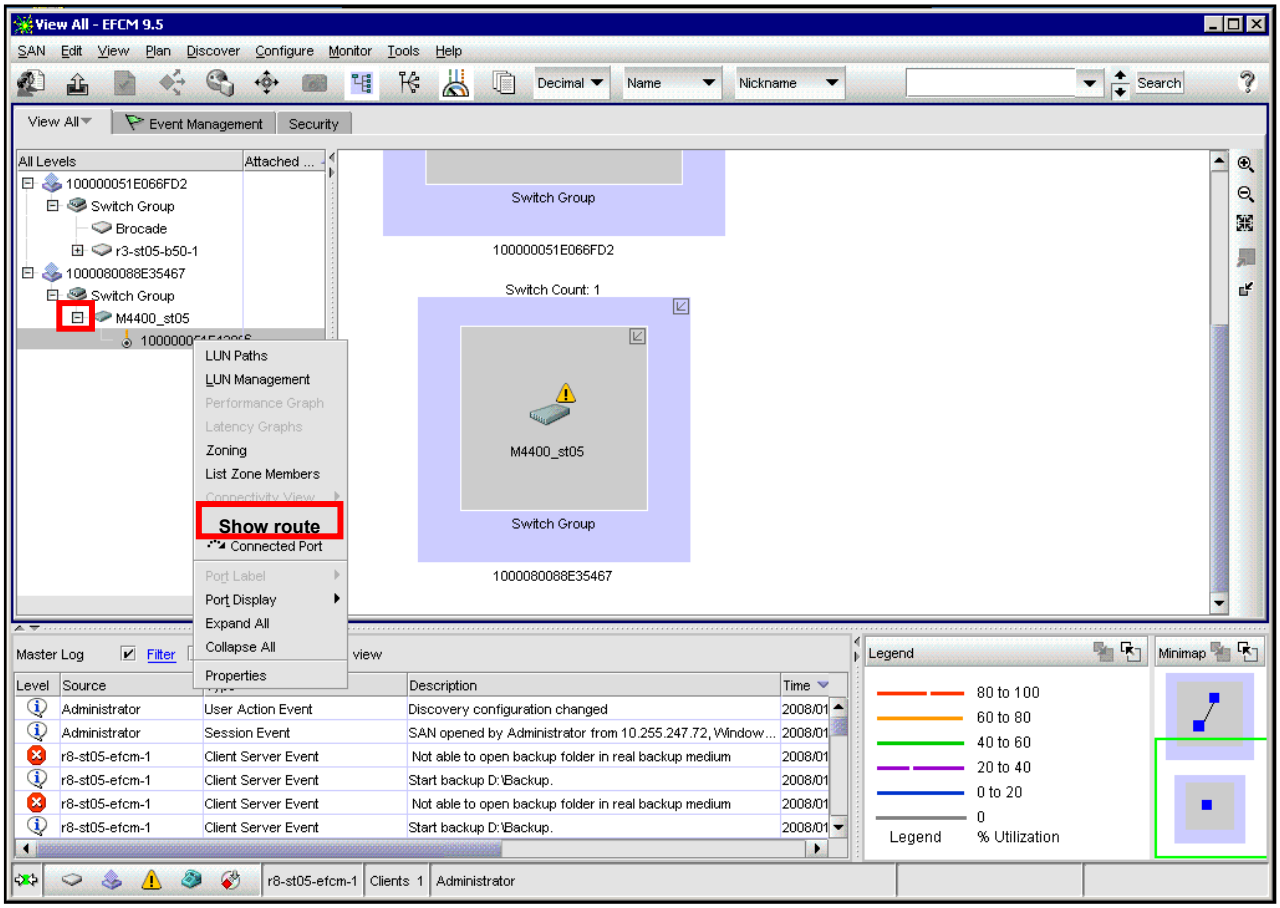

Figure 1: EFCM Routing

SHOWING ROUTES BETWEEN TWO END-PRODUCTS

NOTE: This feature is only available for fabrics consisting solely of manageable products

You can use the Show Route feature to view the path that Fibre Channel frames must take between two end-products in a multi-switch fabric. If you intend to show a different route within the same fabric, the previous route is automatically hidden.

© 2008 Brocade Communications Systems, Incorporated.

REQUIREMENTS

To view the route between two products, the following conditions must be met:

- There must be two or more switches in the fabric
- All switches or Directors in the route must be managed by the application and attached to the same server
- All switches or Directors in the route must be manageable products and must be running firmware version M-EOS 7.0 or higher
- All attached products in the route must be in the same zone

PROCEDURE TO SHOW ROUTES IN EFCM

To show the route for two specific ports on the end nodes, perform the following steps:

1. In the Product List, click the **+** next to a switch product icon to see the nodes
2. Right-click a node and select *Show Route*
3. The *Show Route* dialog box displays
4. Select a destination node from the *Destination Port* table
5. Click *OK*. The route between the nodes displays on topology

© 2008 Brocade Communications Systems, Incorporated.

EFCM GROUP MANAGER

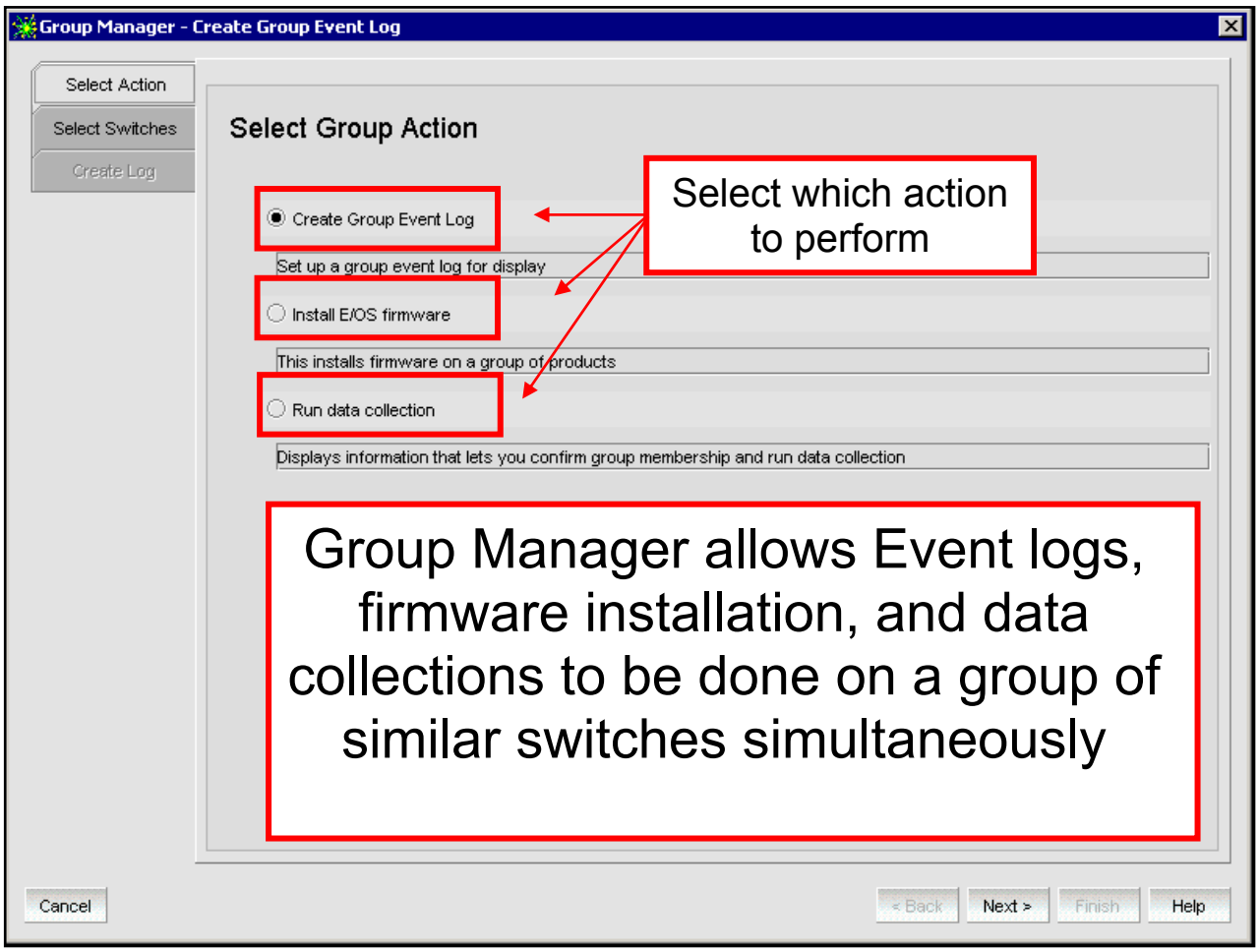
Group Manager - Create Group Event Log
Select Action
Select Switches
Create Log
Select Group Action
Select which action to perform
Create Group Event Log
Set up a group event log for display
Install E/OS firmware
This installs firmware on a group of products
Run data collection
Displays information that lets you confirm group membership and run data collection
Group Manager allows Event logs, firmware installation, and data collections to be done on a group of similar switches simultaneously
Cancel
< Back
Next >
Finish
Help

Figure 2: EFCM Group Manager

Group Manager can be used to define logical groups, not necessarily groups that are dependent on a selected task. For example, you can create a group with all the switches in the fabric, even if the Group Manager is unable to perform the current task on all the members of the group. A status message will display if the task is not supported for one or more members of the group. To perform any action from the Group Manager, the following conditions must exist:

- The SAN management application must be set up to manage the switch or Director
- The switch or Director must support the Element Manager option

© 2008 Brocade Communications Systems, Incorporated.

ESCM HBA MANAGEMENT TOOL

With ESCM you can:

- Collect event logs
- Manage HBA firmware upgrades
- Access the Boot BIOS
- View port statistics including error statistics
- Manage remote hosts (Import HBAs from other hosts)
- Perform diagnostics
- Configure device persistence
- Access the HBA via a GUI or CLI

ISCSI

- The FC4-16IP blade is the only device that runs the iSCSI protocol
- Allowed access is from iSCSI initiators to Fibre Channel targets only
- It can be monitored by Fabric Manager

MONITORING THE HEALTH OF A SAN

There are many tools available to monitor the health of a SAN:

- SAN Health
- Fabric Manager
- EFCM
- Fabric Watch (constant monitoring, as that is it's purpose)

© 2008 Brocade Communications Systems, Incorporated.

MONITORING B-SERIES SWITCHES

- Use `pathinfo`, `topologyshow` or `urouteshow` to visualize the fabric
- Use `porterrshow` and `portstatsshow` to see if there are any port errors / discarded frames. Note: These are just counters so you would need a set of logs, duplicate the problem and then capture a second set of logs to determine if the errors are incrementing at the time the problem was happening
- Use `portperfshow` / APM to see the I/O (must be captured during the time of the problem). If the switch has APM Web Tools, Fabric Manager or CLI can be used to capture end-to-end performance data
- Fabric Watch can be used to set thresholds to see ISL hot spots and send SNMP alerts. What also makes this tool useful is it can be used to constantly monitor the fabric
- SAN Health can be also be used to look for hot spots and I/O over time; it also tells you if you have a zoning configuration enabled

MONITORING M-SERIES SWITCHES

- SAN Routing: EOSdc -> RTM_Flow_01 file can be used to draw out the fabric
- Port Statistics log can be used to look at port errors / discarded frames. As with the B-Series switches these are just counters so a before and after set of logs would be required to determine is the error counters are increasing. LIN log can be looked at for link/port issues
- Performance reports (using EFCM Standard or EFCM Enterprise can be run to look at I/O rates on ports.
- Thresholds can be set to determine ISL hot spots
- BB Credits: EOSdc -> PortModules files can be used to look at BB-Credit counters. Note: M-i10K only: When **Remote Fabric** license is enabled, a 1 Gbit/sec, 2 Gbit/sec or 10 Gbit/sec port can be configured from 1 to 1373 BB_Credits

© 2008 Brocade Communications Systems, Incorporated.

FABRIC MANAGER

Fabric Manager is a GUI based application that allows monitoring and management of an entire SAN from one central location

Fabric Manager

- Has the ability to get high-level or detailed information about fabrics, switches and ports
- Launches Brocade Web Tools and related services, as needed, for detailed switch information
- Assists SAN administrators by centralizing the configuration, monitoring and management tasks of SANs
- Reduces the overall cost of SAN management by simplifying management tasks
- Enables firmware download and change management across multiple switches and fabrics
- Provides rapid access to SAN information across Brocade-based SANs
- To install Fabric Manager you must have the correct license and serial number for the number of managed domains. Options include:
    - 4 Domain Limit
    - 10 Domain Limit
    - Unlimited Upgrade (4 domain to unlimited)
    - Unlimited Upgrade (10 domain to unlimited)
    - Unlimited Upgrade (Fabric Manager 4.x unlimited to Fabric Manager 5.x unlimited)
    - 10 Domain Limit Upgrade Version (4 to 10 domain)
    - 4 Domain Limit Upgrade (Fabric Manager 4.x with 4 domains to Fabric Manager 5.x with 4 domains)
    - 10 Domain Limit Upgrade (Fabric Manager 4.x with 10 domains to Fabric Manager 5.x with 10 domains)

FABRIC MANAGER DISCOVERY

You may use a subnet scan to determine all of the devices in a fabric, or enter the IP address of one of the switches in a fabric to start.

© 2008 Brocade Communications Systems, Incorporated.

FABRIC MANAGER CHANGE MANAGEMENT

Fabric Manager *Change Management* provides a common interface to monitor and manage changes to a Fabric Manager SAN *Profile*

- Tracks changes to a range of SAN components
- Checks for changes against a previously-created Fabric Manager baseline
- Notifies you when changes are detected

You can review detailed *reports* of all detected changes

A Change Management profile has three components:

1. A *snapshot configuration* that defines which items to monitor: ISLs, switches in/out, switch configuration, zoning, name server, firmware version, licenses, ports*, device links*, security mode, and security policies.

* *Ports* – Fabric Manager can monitor the status of a designated set of ports. Fabric Manager tracks four status levels: disabled (not configured), offline, online, and down. The mapping of `switchshow` status values to these levels are:

- `lock_ref, port_flt, no_sync, laser_flt, testing` → `down`
- `no_port, disabled, no_module, no_card` → `disabled`
- `no_light, in_sync` → `offline`
- `online` → `online`

* *Device links* – Fabric Manager monitors the switch domain and port WWN to which a device is connected

2. A user-specified *schedule* for automatically checking one or more fabrics against the baseline snapshot

Specify a time interval for checking the items defined in the snapshot

Can compare a single live, or two previously-captured, snapshot(s) against a baseline snapshot

Note: If you schedule more than 4 automated checks at the same time, Fabric Manager will put them in a queue and run 4 checks at one time.

3. A *notification configuration* that defines the response when changes are detected

Sends email notification

Generates a Fabric Manager alert

Auto-generates an XML change report (similar to call home functionality)

© 2008 Brocade Communications Systems, Incorporated.

3 REPORTING AND DOCUMENTATION

3.1 SAN DOCUMENTATION

SAN documentation comes in many forms. The various manuals give relevant information. Some examples include:

- Fabric OS Administrator Guide
  - Information on FCIP
  - Information on zoning
  - Information on routing & trunking
- Fabric OS Command Reference Guide
  - Help files for all of the Fabric OS commands
- Fabric OS MIB Reference Guide
  - Useful topics on installing MIBs and working with SNMP traps
- Fabric OS Message Reference
  - Lists the error messages
- Fabric Watch Administrator's Guide
  - Helps you configure and maintain Fabric Watch threshold monitoring
- Data Center Ready Compatibility Matrix
  - A living document that shows what products are currently qualified by Brocade
- SAN Health is a tool, and also a form of documentation from the reports generated
- EFCM Standard is a tool, and also a means to generate information about M-Series environments
- Fabric Manager is a tool, and also a means to generate information about B-Series environments

© 2008 Brocade Communications Systems, Incorporated.

3.2 TOOLS TO DOCUMENT A SAN

TOOLS

- EFCM Standard
- EFCM Enterprise
  - The Advanced Module will give you performance information
- Fabric Manager
  - Configuration Manager (for configuration files)
  - Physical Inventory Report (does not include the AP7420's XPath OS and virtual switches)
  - Can launch SAN Health
- SAN Health
  - You need Microsoft Visio and Excel to view reports
  - You will get extensive reports and documentation about ports, zoning, performance and more
  - A data capture must be done and then a `.bsh` file is uploaded to Brocade

© 2008 Brocade Communications Systems, Incorporated.

4 TROUBLESHOOTING

4.1 METHODS & TOOLS FOR TROUBLESHOOTING AND DATA GATHERING

TROUBLESHOOTING ROUTERS

As you begin sharing devices, display the FC router resources available with `fcrresourceshow`

```
NDA-T01-7500:admin> fcrresourceshow
      Daemon Limits:
                          Max Allowed         Currently Used
                          ----------------------------------
      LSAN Zones:               3000                    2
      LSAN Devices:            10000                    4
      Proxy Device Slots:      10000                    2

                          WWN Pool Size            Allocated
                          ----------------------------------
      Phantom Node WWN:         8192                  444
      Phantom Port WWN:        32768                  894
      Port Limits:
      Max proxy devices:  2000
      Max NR_Ports:       1000
      Currently Used (column 1: proxy, column 2: NR_Ports):
        4   |      2          1
        5   |      2          1
        6   |      2          1
```

It is important to note that, when troubleshooting routed SANs, some commands relate specifically to switches, and others relate specifically to routers. Switch centric commands would include all the normal FOS commands, some of which have been updated to include pertinent edge fabric information. The `fabricshow` command, for instance, displays all front and translate domains in the edge fabric. Router centric commands, for the most part, start with “fcr”, like `fcrresourceshow`, and display information specific to the routers, and the backbone fabric.

In the `fcrresourceshow` command output, you can see the per-backbone and per-port maximums for the following FC Routing resources:

- LSAN zones
- LSAN devices (proxy or physical devices)
- Proxy device slots (device-to-AL_PA mappings)
- Phantom node WWNs
- Phantom port WWNs (includes ports connecting front and translate domains (*virtual ISLs*), translate domain ports for proxy devices, and EX_Port(s)
- NR_Ports (stored at every physical port for routing decision purposes)

The scalability limits *always* override the maximum values in this command output.

© 2008 Brocade Communications Systems, Incorporated.

For device sharing related issues, two commands are very useful. Use the `switchshow` command on the edge fabrics to verify devices are online:

```
NDA-T01-48K:admin> switchshow | grep e-port -i
116   10    4   0a7400   id N2  Online   E-Port  50:00:51:e3:78:a8:5e:0a "fcr_fd_4"
(downstream)(Trunk master)
117   10    5   0a7500   id N2  Online   E-Port  (Trunk port, master is Slot 10 Port  4 )
118   10    6   0a7600   id N2  Online   E-Port  (Trunk port, master is Slot 10 Port  4 )
```

<Truncated Output>

Use the `cfgshow` command on the edge fabrics to verify device connectivity:

```
NDA-T01-48K:admin> cfgshow
```

<Truncated Output>

```
Defined configuration:
  zone:  fabAzone b48_w2k; b48_disk1
  zone:  lsan_fabBB_fabA b48_disk1; b75_w2k
```

<Truncated Output>

Note: The `zoneshow` command will give the same information in slightly different format

FABRIC MERGE ERRORS

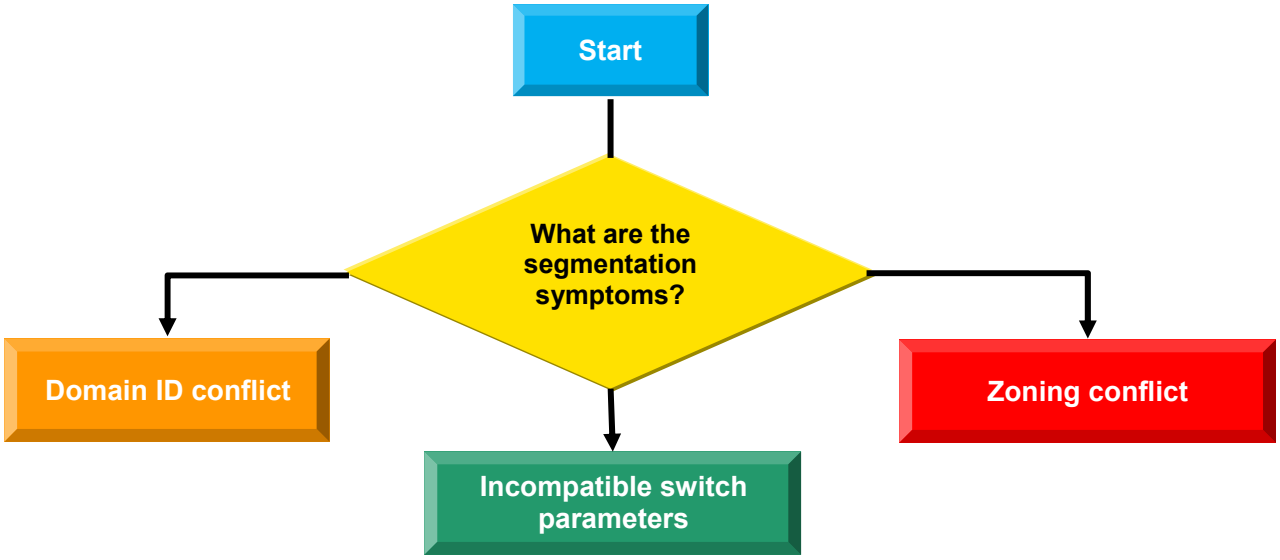

Figure 3: Fabric Merge Troubleshooting Tree

© 2008 Brocade Communications Systems, Incorporated.

SAMPLE FABRIC MERGE ERROR MESSAGES

Domain ID Conflict error message:

```
2007/12/27-14:38:37, [FABR-1014], 8517, FFDC, ERROR, r3-st02-b20-1, Port 8 Disabled: Insistent
Domain ID 1 could not be obtained.  Principal Assigned Domain ID = 2
```

Even though this message states the Principal Assigned DID is assigned 2, if the persistent DID is set it cannot change and therefore segments from the fabric

Incompatible Fabric Parameters error message:

```
2007/12/27-14:45:32, [FABR-1001], 8533,, WARNING, r3-st02-b20-1, port 9, incompatible flow control
parameters (2)
```

Fabric parameters must match

Zoning Conflict error message:

```
2007/12/27-14:59:01, [FABR-1001], 8542,, WARNING, r3-st02-b20-1, port 8, Zone Conflict
```

A merge is not possible if any of the following conditions exist:

- **Configuration mismatch** - Zoning is enabled in both fabrics and the zone configurations that are enabled are different in each fabric
- **Type mismatch** - The name of a zone object in one fabric is used for a different type of zone object in the other fabric
- **Content mismatch** - The definition of a zone object in one fabric is different from the definition of zone object with the same name in the other fabric

© 2008 Brocade Communications Systems, Incorporated.

COLLECTING INFORMATION FOR TROUBLESHOOTING

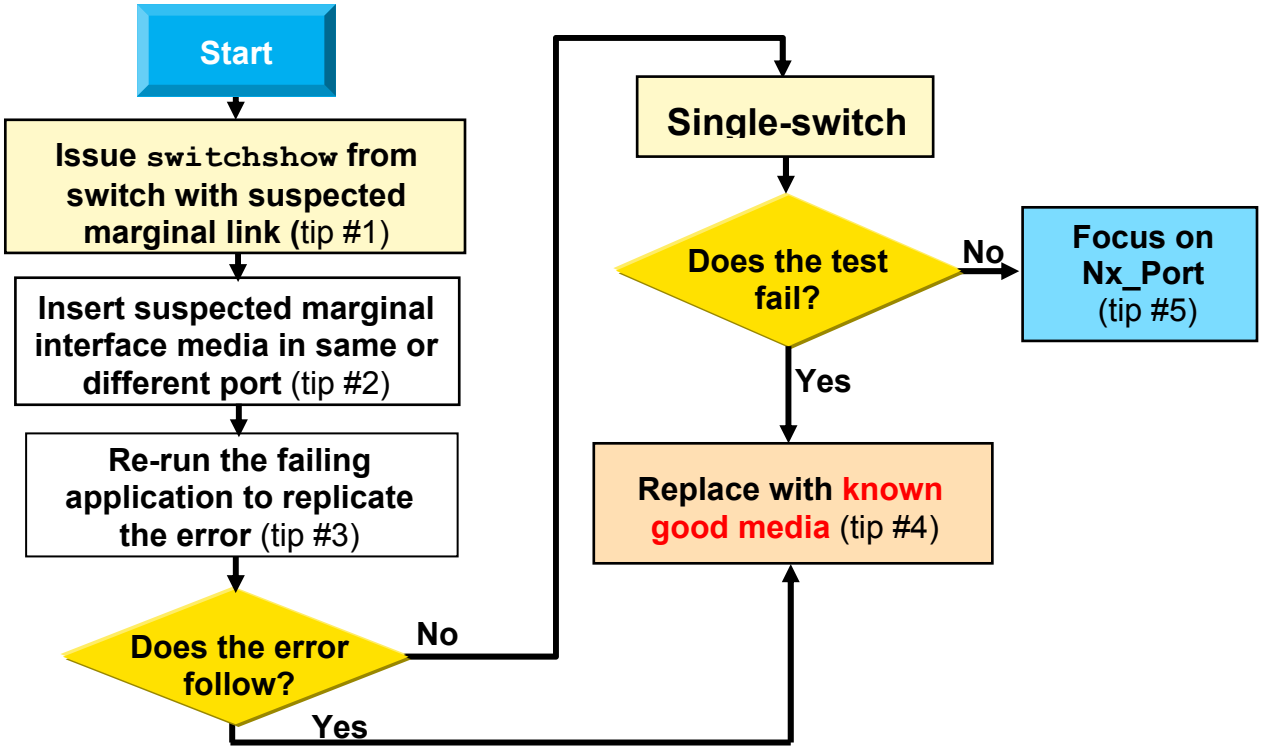
Start
Issue switchshow from switch with suspected marginal link (tip #1)
Insert suspected marginal interface media in same or different port (tip #2)
Re-run the failing application to replicate the error (tip #3)
Does the error follow?
No
Yes
Single-switch
Does the test fail?
No
Focus on Nx_Port (tip #5)
Yes
Replace with known good media (tip #4)

Figure 4: Marginal Link/Port Fault Troubleshooting Tree

Tip #1 – Configure Fabric Watch to capture events on the port in question; capture a `supportsave` to collect information. The `supportshow` (within the `supportsave` would have the following outputs which are useful for troubleshooting these type of issues: `swtichshow`, `portshow`, `porterrshow`, `portcfgshow`, `errdump`, `portlogdump` and `diagshow`. M-EOS switch data collection: Product Info, Port Statistics, Event, LIN and Embedded Port logs.

© 2008 Brocade Communications Systems, Incorporated.

The `fcping` command can also be used to identify a marginal link. Issue `fcping` from the switch with the questionable connection; use WWN of questionable device as the source and look at the response times, consider using the length and number of frame operands to send more data. If you have a marginal connection and send enough frames and/or data you should be able to catch responses with a much longer response time:

```
NDA-ST03-B48:admin> fcping 10:00:00:00:c9:27:22:82 22:00:00:04:cf:bd:58:18
Source:         10:00:00:00:c9:27:22:82
Destination:    22:00:00:04:cf:bd:58:18
Zone Check:     Zoned
Pinging 10:00:00:00:c9:27:22:82 [0x30c00] with 12 bytes of data:
received reply from 10:00:00:00:c9:27:22:82: 12 bytes time:501 usec
received reply from 10:00:00:00:c9:27:22:82: 12 bytes time:449 usec
received reply from 10:00:00:00:c9:27:22:82: 12 bytes time:473 usec
received reply from 10:00:00:00:c9:27:22:82: 12 bytes time:440 usec
received reply from 10:00:00:00:c9:27:22:82: 12 bytes time:444 usec
5 frames sent, 5 frames received, 0 frames rejected, 0 frames timeout
Round-trip min/avg/max = 440/461/501 usec …<truncated output>…
```

Possible responses to the `fcping` are: `reply`, `time out` (which indicated that the attached device does not respond to the ELS echo frame request that is used by `fcping`), or `fcping`: `Error destination (or source) wwn invalid`. This last response occurs when the device is not online or cannot be discovered online.

Tip #2 – Interface media consists of an SFP or Fibre Channel cable. Remove and reinsert interface media. Move interface media to a different port. Use `porterrshow` statistics to determine most likely interface media to move.

Tip #3 – If the original marginal link error was not initiated by I/O activities or POST, then run `porttest` to verify. While `porttest` is running, check the LLI statistic counts via `errshow`, `porterrshow` or `portshow` command outputs.

Tip #4 – Always verify that the new media is "known good". If the error was not initiated by I/O activities or POST, then run `porttest` to verify correction.

Tip #5 – You have isolated the problem, it is the Nx_Port (HBA or storage controller card). Use the Nx_Port utilities to troubleshoot this problem. You may need to verify with the latest HBA/controller driver before replacing the device. Check the vendor compatibility matrix if it is not a Brocade HBA.

© 2008 Brocade Communications Systems, Incorporated.

4.2 IDENTIFYING INFORMATION REQUIRED FOR PROBLEM ESCALATION

ESCALATIONS

Data must be gathered for problem escalation, depending upon the type of situation. In the case of switches, Directors and routers, the bulk of the information should be gathered with `supportsave`, along with a detailed problem description. Other pieces of information would include core files, panic dump output and the output from `supportshow`, which are all part of `supportsave`. When dealing with hosts, detailed information about the host, the ESCM event log and the HBA would be extremely helpful.

If the switch is acting erratically, or devices can no longer see one another, copies of the current and prior configuration files would also be very useful for a support organization. Switch events should also be captured, using these tools:

- SNMP
- RASlog or syslog
- Running CLI commands

SAN CHANGES

If you are making changes to the SAN in the form of adding new switches, data should be gathered by using these tools:

- SAN Health
- EFCM Standard
- Fabric Manager

© 2008 Brocade Communications Systems, Incorporated.

5 SAN MONITORING

5.1 IDENTIFYING TOOLS TO MONITOR A SAN

GATHERING REAL-TIME PERFORMANCE

Tools for B-Series switches:

- EFCM Enterprise
- Web Tools
- Fabric Manager

Tool for M-Series switches:

- EFCM Enterprise

MONITORING ISL UTILIZATION

To monitor ISLs to make sure they are performing within expected boundaries:

- EFCM Standard & Enterprise
- Fabric Manager
- Fabric Watch

THRESHOLDS

On a B-Series switch, Fabric Watch will deliver information about thresholds, using the triggered option.

On an M-Series switch, EFCM Enterprise with the Performance Monitor License will deliver information about thresholds.

END-TO-END PERFORMANCE MONITORING IN A B-SERIES FABRIC

To monitor the end-to-end performance between an initiator and a target for a B-Series fabric some of these products could be used:

- Web Tools
- Fabric Manager
- Advanced Performance Monitor

SNMP

SNMP is a popular way to gather information about alerts and problems in a network. On a SAN, SNMP can be put to use to discover faults and problems, through the use of traps, which are messages from SNMP agents (the switches).

SNMP must be configured on the switch to work within the network framework:

- Obtain the appropriate MIBs
- Configure SNMP on the switch, then trap capabilities and recipients
- Set community strings or SNMP authentication depending upon the SNMP version in use

© 2008 Brocade Communications Systems, Incorporated.

5.2 HOW TO MONITOR AND MANAGE SHARED DEVICES BETWEEN EDGE FABRICS

DOMAIN MANAGEMENT

It is important to keep track of domains in a routed fabric environment. Look at this diagram of a routed fabric:

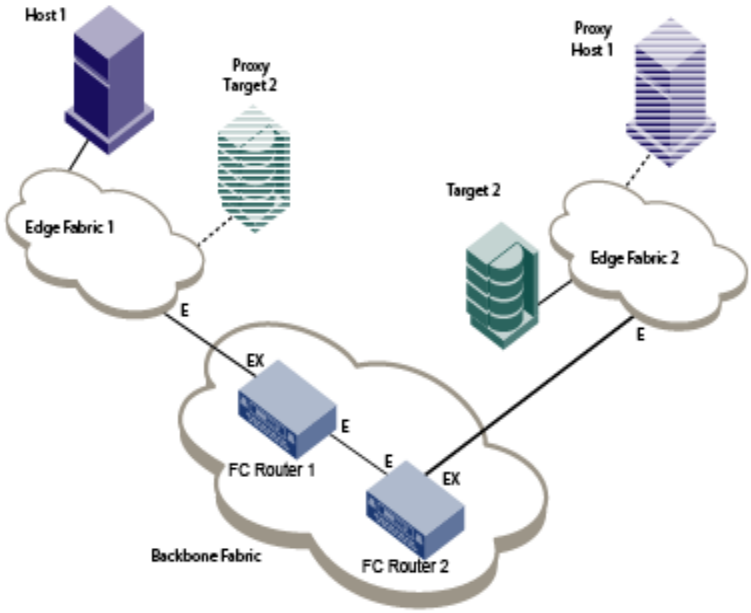

Figure 5: Sample Routed Fabric

The EX_Ports on each router will generate a front domain, and proxy devices will generate a translate domain.

Phantom Front Domain (fd): A *logical domain* created when edge fabrics are connected to backbone fabrics. Starting with Fabric OS v5.2, only a single fd is created for all IFL connections between a router and a particular edge fabric.

Phantom Translate Domain (xd): A logical domain created when routed fabrics share devices. This sharing is accomplished through the creation and enabling of LSAN zones. This logical domain is where the imported devices logically exist.

CONGESTION

Congestion in a routed fabric is handled much the same as in a non-routed fabric:

- Localize devices if possible (although in routed fabrics this may be somewhat more difficult)
- Add IFLs between the edge fabrics and the routers
- Add ISLs between the switches in the backbone fabric

© 2008 Brocade Communications Systems, Incorporated.

VERIFYING DEVICE CONNECTIVITY

Use the `cfgshow` command on the edge fabrics to verify device connectivity:

```
NDA-T01-48K:admin> cfgshow
<Truncated Output>
Defined configuration:
  zone:  fabAzone b48_w2k; b48_disk1
  zone:  lsan_fabBB_fabA b48_disk1; b75_w2k
<Truncated Output>
```

The `zoneshow` command will give the same information in slightly different format

You may also use Fabric Manager, as long as you use the MetaSAN View

VERIFYING PROXY DEVICES

Display proxy devices with the `fcrproxydevshow` command:

```
NDA-T01-7500:admin> fcrproxydevshow

  Proxy            WWN             Proxy      Device    Physical    State
 Created                            PID       Exists      PID
in Fabric                                    in Fabric
--------------------------------------------------------------------------------
    10   10:00:00:00:c9:2b:4e:bc  01f001      100       010c00    Imported
   100   22:00:00:04:cf:bd:56:53  02f001       10       0a0fe2    Imported
Total devices displayed: 2
```

Note: Besides using CLI commands to verify devices, ports, zones, proxies, etc., verification can be achieved using SAN Health and Fabric Manager

M-SERIES ROUTERS

Monitoring an M-Series routed fabric requires the use of EFCM Standard. Under the Configuration Archive dialogue box, you may choose to archive some files that will help in the event of a problem. You would want to save copies of the event log and take a backup of the configuration, in the event something happens that requires the information from a point in time.

To manage routing within an M-Series fabric consider these zoning caveats:

- Only the active zone set is distributed to the switches in the fabric
- Depending on the platform, membership is restricted either by zone set size or member count

© 2008 Brocade Communications Systems, Incorporated.

5.3 HOW TO MONITOR AND MANAGE DEVICES

EFCM AND ZONING IN M-SERIES FABRICS

It is necessary to have the Zoning Module in EFCM to manage zoning.

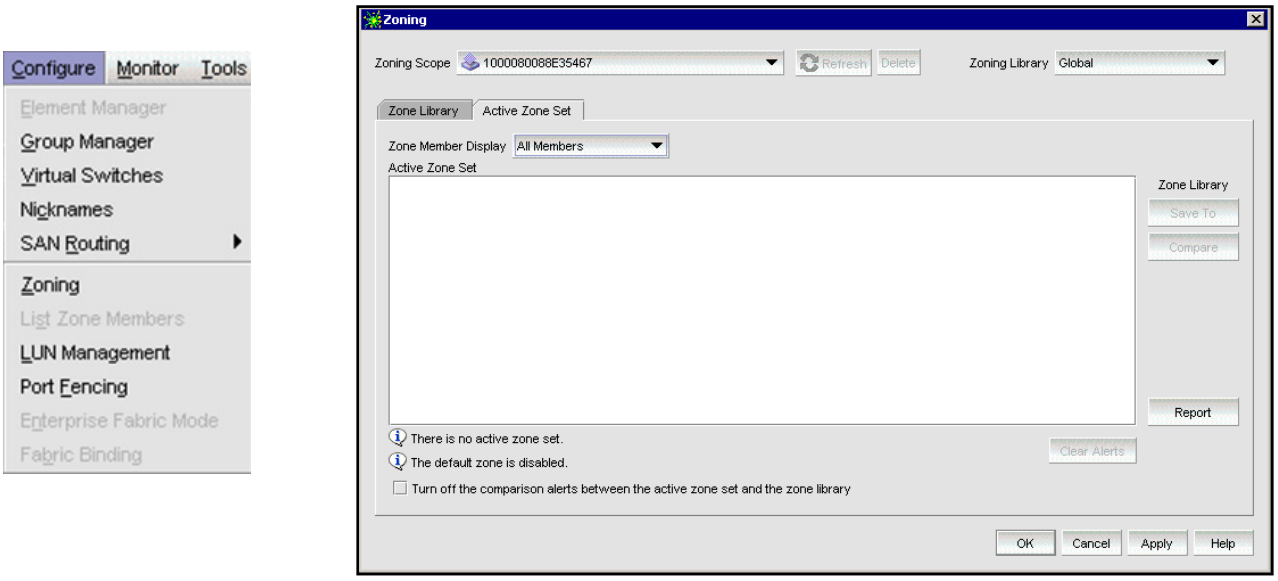

Figure 6: Active Zone Set Tab in EFCM

Zone and Zone Set naming conventions:

- Names are NOT case sensitive
- Names cannot begin with “SANav_” or “SMP”. These prefixes are reserved. Any M-Series switch having a zone beginning with a reserved prefix will not be discovered.
- Names cannot begin with a number
- Recommended maximum character limit is 60 characters
- No duplicate names are allowed between zones or zone sets in the same zone library

It should be noted that EFCM can also manage zoning in a B-Series fabric as well.

© 2008 Brocade Communications Systems, Incorporated.

ZONING IN A B-SERIES FABRIC

Some best practices:

- Monitor the zoning database size
- Keep to a standard naming convention
- Manage zoning from the latest Fabric OS revision switch
- Keep 1 HBA/zone
- Zone using a core switch over an edge switch
- Manage zoning from user accounts that have admin, zone admin and fabric admin privileges

MANAGING AN HBA

The ESCM utility can be used to manage a Brocade-branded HBA. To download firmware to an Emulex HBA, you may use Fabric Manager. The HBA must be FDMI compliant, and make sure that FDMI is enabled.

MONITORING ISL TRAFFIC

Traffic on the ISLs can be monitored with these tools:

- Advanced Performance Monitor
- Fabric Watch
- SAN Health
- Web Tools
- `portperfshow`
- EFCM

© 2008 Brocade Communications Systems, Incorporated.

© 2008 Brocade Communications Systems, Incorporated.

6 SAN CONFIGURATION

6.1 MANAGING FICON FABRICS

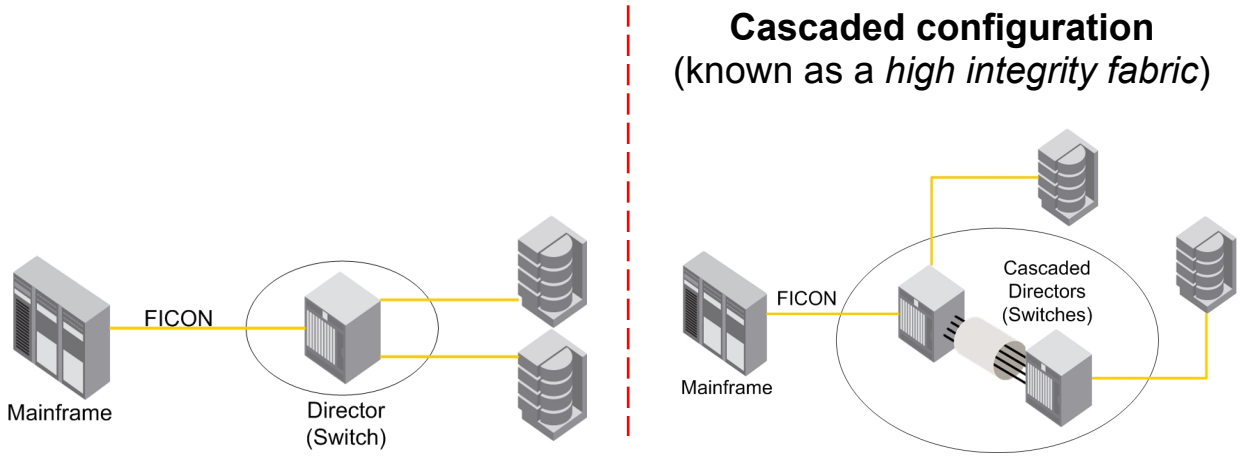

Figure 7: Supported FICON Topologies

SINGLE DIRECTOR REQUIREMENTS

No licenses are required unless two-byte addressing is used. Most customers are not cascading and therefore only use single-byte addressing

Even though not required, Insistent Domain ID (IDID) should be set

- IDID guarantees that a switch operates only with its pre-assigned domain ID

CASCADED DIRECTOR REQUIREMENTS FOR M-SERIES

Requires a SANtegrity license for 2-byte addressing

Enable Enterprise Fabric Mode in EFCM which will enable:

- Fabric binding (mandatory)
- Insistent Domain ID (IDID) (mandatory)
- Switch binding (optional)

All fabric parameters must be the same

© 2008 Brocade Communications Systems, Incorporated.

CASCADED DIRECTOR REQUIREMENTS FOR B-SERIES

Requires Secure Fabric OS License

- Includes fabric binding, switch binding, and port binding security methods that prevent unauthorized devices from joining a fabric

Switch Connection Control (SCC) Policy in Security Set

- SCC policy is used to restrict which switches can join the fabric

Insistent Domain ID (IDID) must be set on all switches

Domain IDs need to be unique

- If both switches have IDID set and the same Domain ID, the fabrics will not merge

Dynamic Load Sharing (DLS) should be set to **Off**.

In-Order Delivery (IOD) should be set to **On**.

The DLS setting is recommended in a FICON environment. It does not allow for recomputing of routes when an F_Port or E_Port changes status. This reduces the number of channel error messages (interface-control checks) generated by the channel subsystem when a change of status occurs in the switch.

The IOD setting is mandatory in a FICON environment. It ensures frames are delivered in order. When frames are not delivered in order, they will be dropped by the switch.

ENABLING CUP

- The CUP License must be installed
- FICON Management Server (FMS) Mode must be enabled

With CUP License installed and FMS Mode enabled

- CUP Port is activated: Frames w/ address ‘0xDDFE00’ are routed to the CPU (CUP port address) and in-band CUP commands processed

© 2008 Brocade Communications Systems, Incorporated.

6.2 PERFORMING ROUTINE MAINTENANCE

MEASURING LATENCY

EFCM may be used to measure latency with the Latency Graphs feature

Latency Graphs show the response time in microseconds (µs) for each LUN communicating with the HBA.

Real time performance data is used to plot the latency graphs.

- Historical data does not exist for latency graphs

Latency is determined by the SCSI inquiry time. A SCSI inquiry is sent from the HBA to the LUN and the time taken to make the round trip is calculated.

Latency graphs are only available for HBA devices when the following conditions are met:

- The HBA is discovered using in-band discovery
- The HBA and the storage device are in the same zone

FIRMWARE DOWNLOADS

When downloading firmware to a device doing FCIP routing, the FCIP links may be interrupted. The Fabric OS will indicate if this going to be the case.

When using Fabric Manager to download firmware consider these points:

- Fabric Manager has a firmware repository
- Firmware may be downloaded to multiple switches simultaneously
- There is a built-in FTP server
- Firmware may be downloaded to FDMI-compliant HBAs

CONFIGURATION FILE UPLOADS

Configuration files should be backed up on a regular basis, and archived in the event of a support issue, or the need to restore zoning, license keys, SNMP, or Fabric Watch settings.

The `configupload` command is used from the CLI on a B-Series switch.

For an M-Series switch EFCM Basic is used.

USING FABRIC MANAGER FOR MAINTENANCE FUNCTIONS

Fabric Manager can be used to backup, restore and replicate configuration files. It can work with these protocols:

- FTP
- FCIP
- HTTP(S)
- iSCSI
- FDMI
- FCP

© 2008 Brocade Communications Systems, Incorporated.

ISL AND TRUNK MAINTENANCE

In order to have fabrics merge there must be some requirements met:

- No duplicate domain IDs
- `fabric.ops` parameters must be the same

In order to have a trunk group form, these requirements must be met:

- Trunking licenses on both switches involved in the trunk
- Trunks must start and end in a port group
- Long distance settings must match
- The maximum cable differential may not be greater than 400m
- The port speeds must match, and cannot be lower than 2 Gbit/sec

© 2008 Brocade Communications Systems, Incorporated.

6.3 MAINTAINING SAN EXTENSION SOLUTIONS

VALIDATE THE IP NETWORK

Verify the IP interface and FCIP tunnel settings with the ipPerf tool and the `portcmd --ipperf [slot]/port` command

- Always specify local GbE port, the source IP (`-s`) and destination IP (`-d`), and whether this port is the sender (`-S`) or receiver (`-R`)
- Start the ipPerf receiver first (`-R`), then start the ipPerf sender (`-S`)
- If no time interval is specified, type **Ctrl-C** on the sender to stop
- Can be run on an active tunnel

The `portcmd --ipperf [slot]/port` command output on the sender displays end-to-end IP path performance values

- Updated in real-time, according to the time and test interval
- Two bandwidth values: BW and WBW

```
B7500:admin> portcmd –ipperf ge0 –s 192.168.23.100 –d 192.168.20.10 –R
ipperf to 192.168.20.10 from IP interface 192.168.23.100 on /0:3227
B48000:admin> portcmd –ipperf 10/ge0 –s 192.168.20.10 –d 192.168.23.100 –S
ipperf to 192.168.23.100 from IP interface 192.168.20.10 on 10/0:3227
30s: BW:118.86MBps WBW(30s): 58.01MBps Loss(%):0.00 Delay(ms):1PMTU:2348
```

<Truncated Output>

As you can see from the command output, jumbo frames are supported from the PMTU.

BW represents what the FCIP tunnel / FC application throughput rather than the Ethernet on the wire bytes.

WBW represents what the FCIP tunnel / FC application throughput rather than the Ethernet on the wire bytes.

Loss (%) is the number of TCP retransmits. This number is an average rate over the last display interval.

Delay (ms) is the TCP smoothed RTT and variance estimate in milliseconds.

Path MTU is the largest IP-layer datagram that can be transmitted over the end-to-end path without fragmentation. This value is measured in bytes and includes the IP header and payload. A value of 2148 or larger indicates that jumbo frames are supported in the network.

In the example above, two switches are connected via FCIP (port ge0 on 7500, and port 10/ge0 on 48000). After creating IP interfaces on the appropriate GbE ports, the ipPerf utility is launched, with 7500 as the receiver, and 48000 as the sender. The command output on each switch notes the “to” and “from” addresses, as well as the slot/port indicator (slot 0 is the motherboard on the Brocade 7500).

As part of the verification, the packet loss and round trip delay can be used to validate that the tunnel is performing as the WAN provider claims.

© 2008 Brocade Communications Systems, Incorporated.

BB CREDITS

Speed	Credits/km	Credits/50 km	Credits/100 km
1	.5	25	50
2	1	50	100
4	2	100	200

Table 3: BB Credits

If you double the speed, or double the distance, you need to double the credits available on the port

If the speed doubles the maximum distance is cut if half

If you double the speed make sure you have the correct SFP for that speed

Starting with the 4 Gbit/sec ASICs, no port will be starved for BB credits. Any port can run in a buffer-limited mode if need be. Also, no one port can take more than 255 credits.

© 2008 Brocade Communications Systems, Incorporated.

6.4 MANAGING ACCESS GATEWAY SOLUTIONS

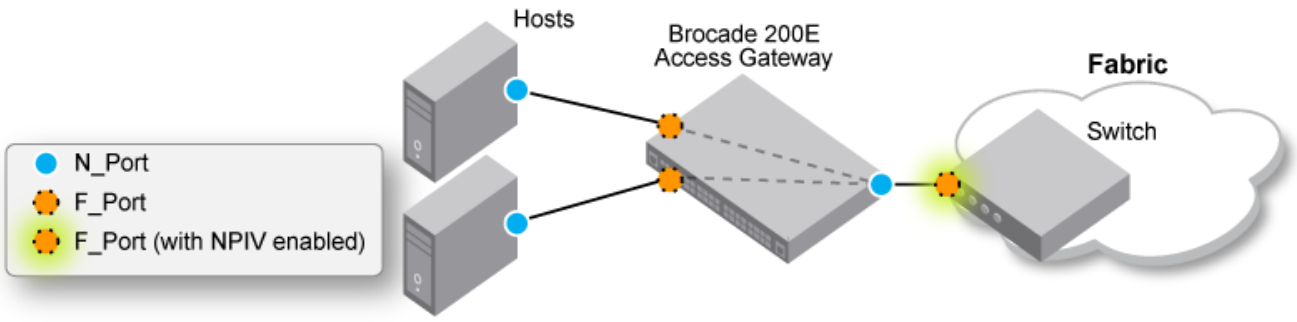

Figure 8: Access Gateway

In Fabric OS v5.3, the Brocade 200E can be configured as an *Access Gateway*

- Access Gateway ports can be configured as N_Ports, which connect to the edge fabric
- No change in domain count – improves the scalability of the fabric
- HBAs are mapped (via NPIV) to the N_Ports, and connect to the edge fabric through the N_Ports – no fabric management or zoning issues

The Brocade Access Gateway allows multiple host bus adapters (HBAs) to access the fabric using fewer physical ports. Instead, certain Access Gateway ports are configured as N_Ports, with the attached hosts mapped through the N_Ports via the N_Port ID Virtualization (NPIV) protocol. The Brocade Access Gateway is a device management tool and provides only a subset of Fabric OS commands, so it does not consume critical fabric elements (e.g. domain IDs) that could inhibit scalability. The Brocade Access Gateway is compatible with different types of fabrics, including Brocade-, Cisco-, and McDATA-based fabrics.

ACCESS GATEWAY DETAILS

Access Gateway is included in Fabric OS v5.3 – no separate license required

Access Gateway is supported on the following GoldenEye-based platforms:

- Switches: Brocade 200E
- Embedded switches: Brocade 4012, 4016, 4020, 4024
- Ports on Demand licenses required for all ports

Attached F_Port devices must be Fibre Channel Protocol (FCP) initiators only

- Not supported: FCP targets, loop devices, FICON channels/control unit connectivity

© 2008 Brocade Communications Systems, Incorporated.

ACCESS GATEWAY PORT MAPPING

A Brocade Access Gateway uses a *port map* to direct traffic from host HBAs to the N_Ports that connect to the fabric

- The port map and N_Port configuration can be edited

Enabling Access Gateway on a Brocade 200E sets a default port map

- N_Ports: Ports 12, 13, 14, 15
- Three F_Ports mapped to each N_Port

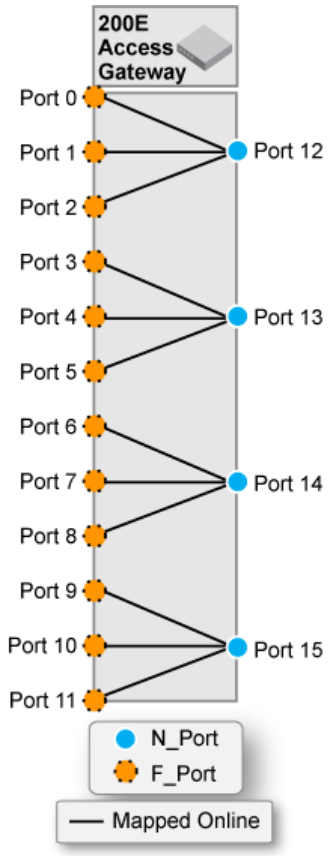

Figure 9: Access Gateway Default Port Map

© 2008 Brocade Communications Systems, Incorporated.

The Access Gateway uses NPIV to assign the 24-bit FC address, based on the port map

- F_Ports/devices share the same domain and area values as the 200E N_Ports to which they are mapped
- The last byte is assigned in the order in which the devices log in to the fabric

Example:

- Port 14 address = 040500
- Host_5 address = 040501
- Host_6 address = 040502

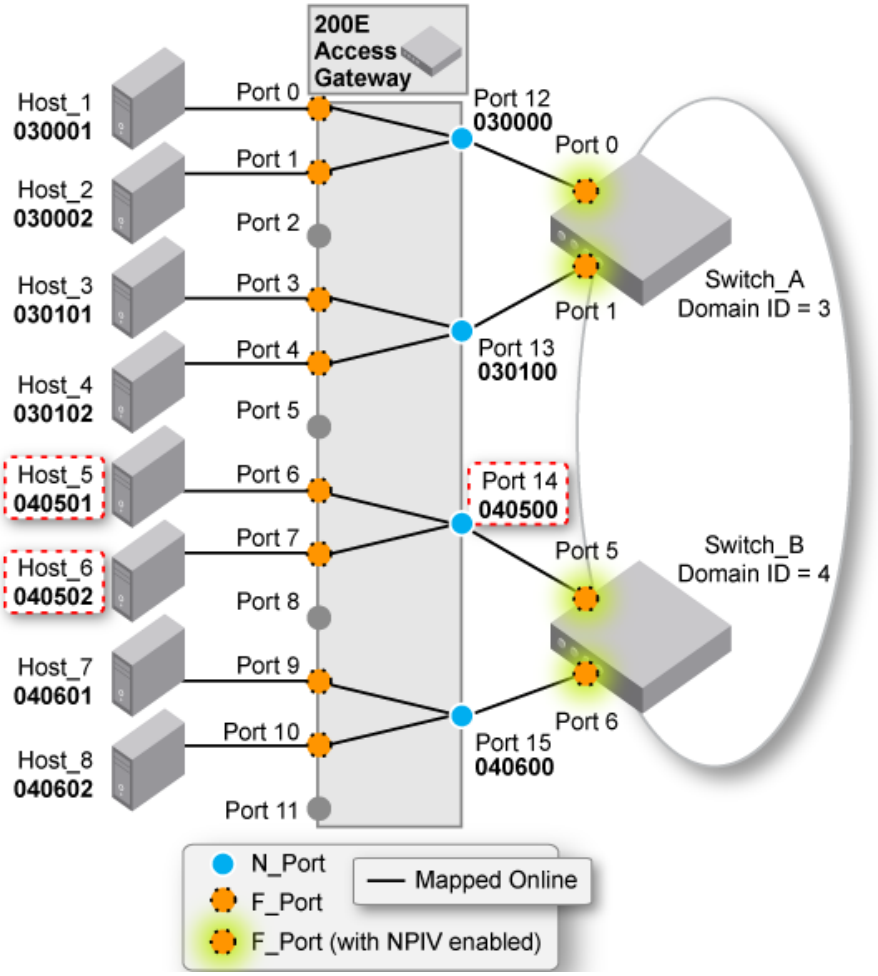

Figure 10: Access Gateway 24-Bit FC Address Assignments

© 2008 Brocade Communications Systems, Incorporated.

7 TAKING THE TEST

Once the test begins, you will first see this screen:

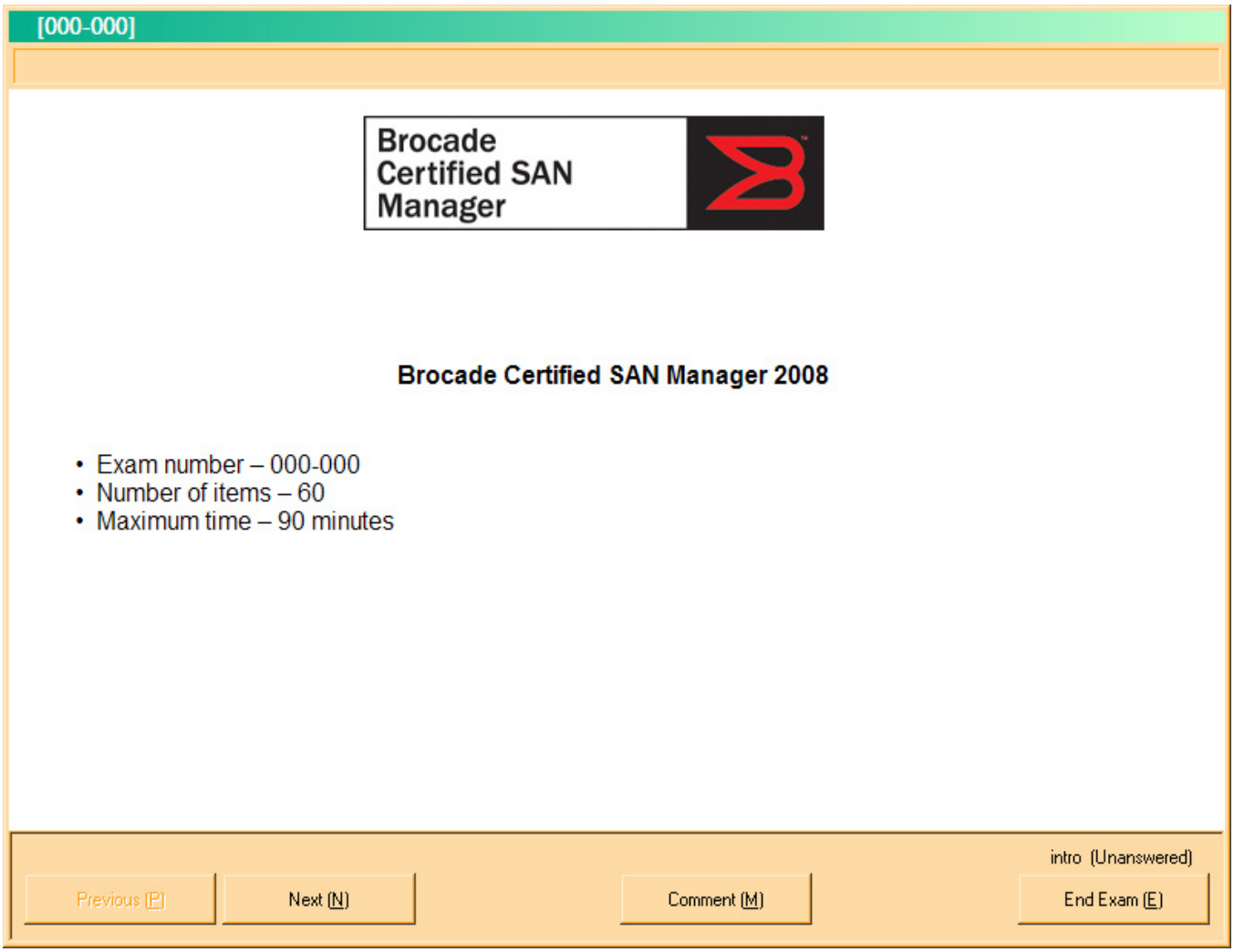

Figure 11: Introduction Screen

© 2008 Brocade Communications Systems, Incorporated.

After the Introduction Screen, once you click on Next, you will see the non-disclosure agreement:

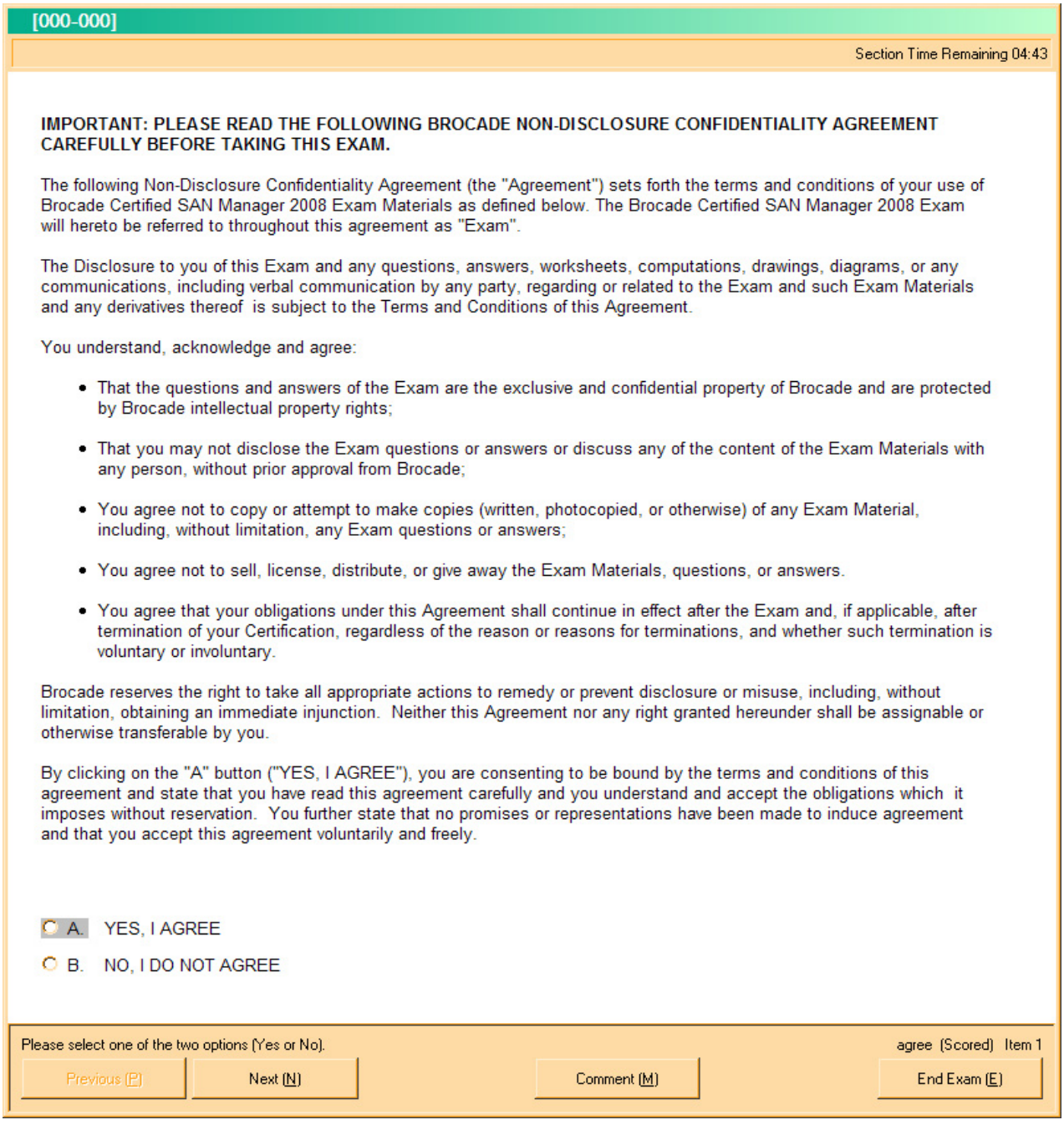
[000-000]
Section Time Remaining 04:43
IMPORTANT: PLEASE READ THE FOLLOWING BROCADE NON-DISCLOSURE CONFIDENTIALITY AGREEMENT CAREFULLY BEFORE TAKING THIS EXAM.
The following Non-Disclosure Confidentiality Agreement (the "Agreement") sets forth the terms and conditions of your use of Brocade Certified SAN Manager 2008 Exam Materials as defined below. The Brocade Certified SAN Manager 2008 Exam will hereto be referred to throughout this agreement as "Exam".
The Disclosure to you of this Exam and any questions, answers, worksheets, computations, drawings, diagrams, or any communications, including verbal communication by any party, regarding or related to the Exam and such Exam Materials and any derivatives thereof is subject to the Terms and Conditions of this Agreement.
You understand, acknowledge and agree:
That the questions and answers of the Exam are the exclusive and confidential property of Brocade and are protected by Brocade intellectual property rights;
That you may not disclose the Exam questions or answers or discuss any of the content of the Exam Materials with any person, without prior approval from Brocade;
You agree not to copy or attempt to make copies (written, photocopied, or otherwise) of any Exam Material, including, without limitation, any Exam questions or answers;
You agree not to sell, license, distribute, or give away the Exam Materials, questions, or answers.
You agree that your obligations under this Agreement shall continue in effect after the Exam and, if applicable, after termination of your Certification, regardless of the reason or reasons for terminations, and whether such termination is voluntary or involuntary.
Brocade reserves the right to take all appropriate actions to remedy or prevent disclosure or misuse, including, without limitation, obtaining an immediate injunction. Neither this Agreement nor any right granted hereunder shall be assignable or otherwise transferable by you.
By clicking on the "A" button ("YES, I AGREE"), you are consenting to be bound by the terms and conditions of this agreement and state that you have read this agreement carefully and you understand and accept the obligations which it imposes without reservation. You further state that no promises or representations have been made to induce agreement and that you accept this agreement voluntarily and freely.
A. YES, I AGREE
B. NO, I DO NOT AGREE
Please select one of the two options (Yes or No).
agree (Scored) Item 1
Previous (P)
Next (N)
Comment (M)
End Exam (E)

Figure 12: Non-disclosure Agreement

© 2008 Brocade Communications Systems, Incorporated.

Once you agree to the terms, then the timed test will begin.

This is a sample of how the questions will look. In this example, you see a multiple-choice question.

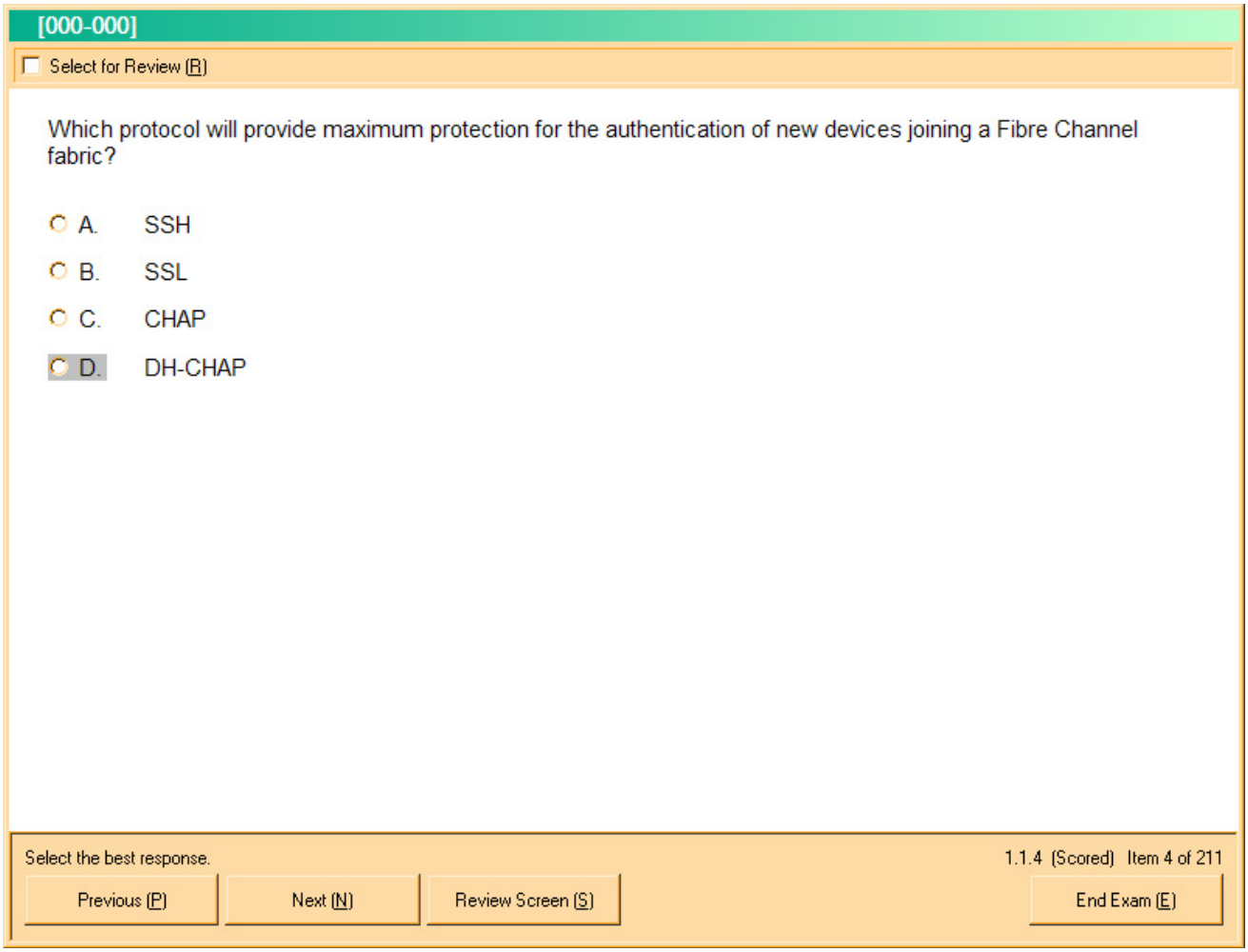

Figure 13: Sample Question

© 2008 Brocade Communications Systems, Incorporated.

When you complete the test, you will see a summary of your results. This summary includes your overall score, as well as your score for each of the six major portions of the exam.

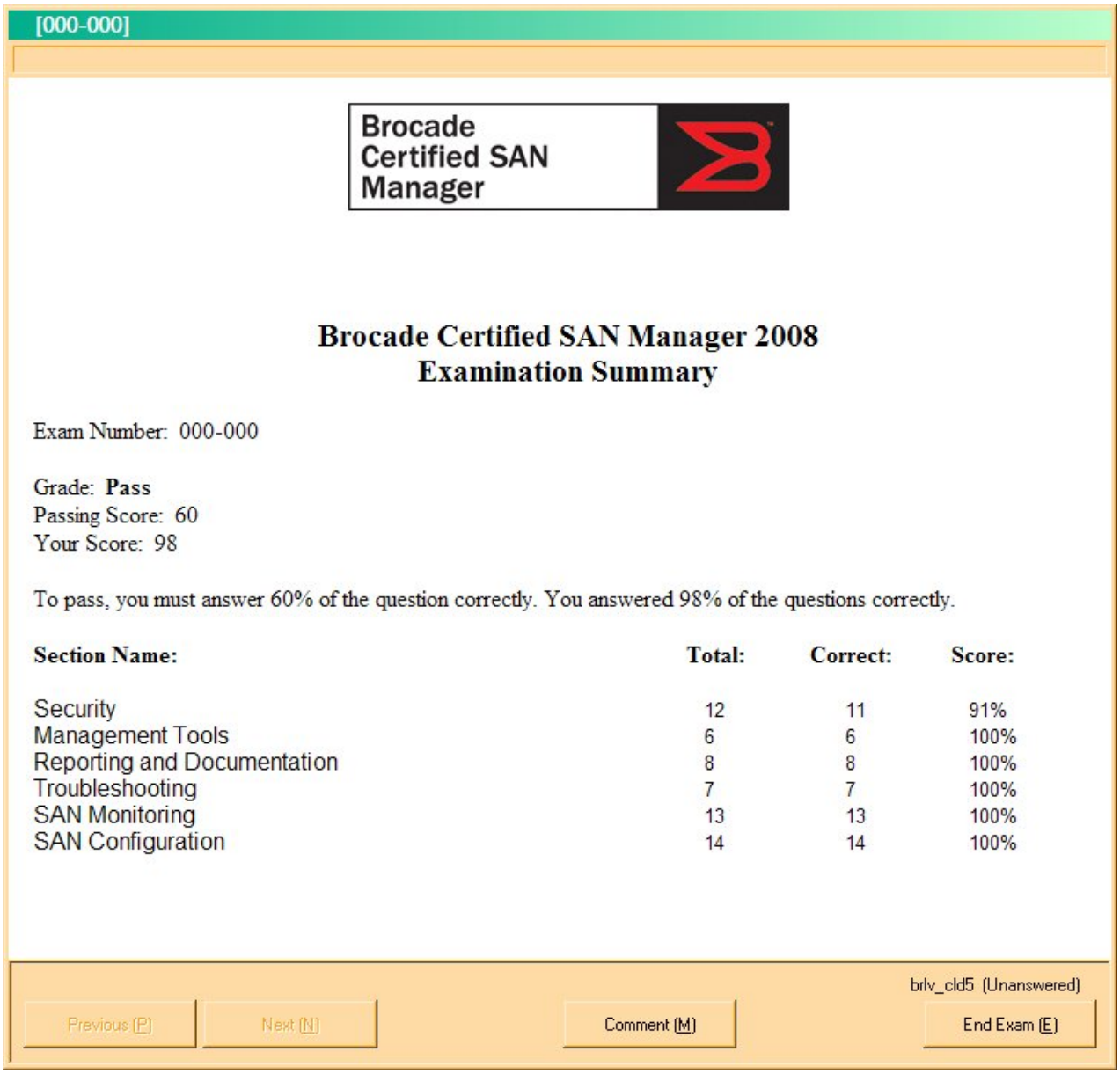

Figure 14: Examination Summary

© 2008 Brocade Communications Systems, Incorporated.